UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/754,713	01/12/2004	Jason Whitman Keith Brothers	062070-0311769	1344

909 7590 09/04/2007

PILLSBURY WINTHROP SHAW PITTMAN, LLP
Eric S. Cherry - Docketing Supervisor
P.O. BOX 10500
MCLEAN, VA 22102

EXAMINER	
PALIWAL, YOGESH	
ART UNIT	**PAPER NUMBER**
2135	

MAIL DATE	DELIVERY MODE
09/04/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/754,713	KEITH BROTHERS ET AL.	
	Examiner	Art Unit	
	Yogesh Paliwal	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07/19/2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

- Applicant's amendment filed on July 19,2007 has been entered. Applicant has amended claims 1-30 and added a new claim 31. Currently claim 1-31 are pending in this application. Any well known art statements made in the prior office action not argued by applicant is taken as admittance of prior art as per MPEP 2144.03.
- Examiner acknowledges clarification of claim language of claims 28-29 for minor informalities. As a result, all claim objections previously presented are withdrawn.
- Examiner acknowledges clarification of claim language of claims 10-15 and 16-22 to overcome rejection under 35 U.S.C. 101. As, results, all rejections under 35 U.S.C. 101 are withdrawn.

Response to Amendment

- Applicant has amended all independent claims, which necessitated new ground of rejection. See rejection below.

Response to Arguments

1. Applicant's arguments filed on 07/19/2007 have been fully considered but they are not persuasive for the following reasons:

- Applicant argues that: "However, Shetty does not security criteria, mechanisms, or any other technique used by the firewall for "blocking one or more subsequently received packets from being transmitted to the target system," as

recited in claim 1, for example. By contrast, Shetty provides additional security on top of the firewall by way of "protocol filters," which scan a data stream for malwares and take "corrective action, for example, by filtering the malware out of the data stream" (e.g., col. 5, lines 27-45)."

- In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "blocking one or more subsequently received packets from being transmitted to the target system,") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Note: This limitation is now present in the claim set after the amendment and a new reference (see below) is found that discloses this limitation. As a result, adding this limitation adding this limitation in all independent claims with other limitation in claims necessitated new ground of rejection.

Claim Objections

2. Claims are objected to because of the following informalities:

- Claim 3, line 3, "a destination a port number", should read, "a destination a port number".
- Claim 23, line 13, "directed at the terminal device packets and", should read, "directed at the terminal device ~~packets~~ and").

- Claim 31, line 3, "a destination a port number", should read, "a destination a port number".

Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 8 and 21 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Currently amended claim 8 recites, "The method according to claim 1, further comprising notifying the source system that the attack has been detected and that packets subsequently sent from source system will be blocked".

Originally filed Specification describe sending a notification to the attacking source at only following two instances:

Paragraph 0025 recites, "According to another aspect of the invention, the target system may notify the attacking source of the detection of the attack and/or indicate that a block was placed on the data packets received from the attacking source. The notification may be enabled through sending a message to the attacking source based

on the IP address of the attacking source extracted from the data packet associated with the known harmful computer codes, preselected identifying information, or other identifying information."

Paragraph 0059 recites, "According to one embodiment of the invention, the target system 105 may notify the attacking source of the detection of the attack and/or indicate that a block was placed on the data packets received from the attacking source". According to one embodiment of the invention, the notification may be enabled through sending a message to the attacking source based on the IP address of the attacking source extracted from the data packet associated with the known harmful computer codes, preselected identifying information, or other identifying information. According to another embodiment of the invention, if the attack is detected via email, the target system 105 may notify the attacking source via a SMTP error response about the reason for the block."

Although above paragraphs describe notifying the source system that the attack has been detected as partially required by amended claim 8, however, examiner was unable to locate in the original description, the additional limitation of notifying the source system "that packets subsequently sent from source system will be blocked", as now recited in amended claim 8. Additionally no figures in original drawing sheets depict this limitation and also no other claim originally filed recites this limitation. Examiner asserts that this additional limitation is recited simply to overcome the reference and has no support in the original disclosure as filed.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 2, 3, 4, 5, 6, 7, 8, 12, 13, 14, 16, 17, 18, 19, 20, 21, 23, 25, 26, 27, 28, 30, 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shetty (US 6,772,345), hereinafter Shetty, in view of Alampalayam et al. (Alampalayam, S.P.; Anup Kumar, "An adaptive security model for mobile agents in wireless networks," Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE , vol.3, no., pp. 1516-1521 vol.3, 1-5 Dec. 2003), hereinafter Alampalayam.

Regarding **Claims 1, 10 and 16**, Shetty discloses a method, system and computer program product for detecting and preventing attacks directed at a target system **(Column 1, lines 6-8, "The present invention relates to a method, system and computer program product for detecting computer malwares that scans network traffic at the protocol level")**, comprising:

receiving one or more packets originating from a source system **(Fig. 1, Numeral 102, "Network Traffic In")**, the received packets directed to the target system **(Fig. 1,**

numeral 104, "Network Traffic Out" and also at Column 1, lines 58-60, "Malware scanning of data that is being transferred or downloaded to a computer system");

monitoring the received packets to identify one or more of the packets that include information associated with a signature of an attack directed at the target system **(Column 1, lines 65-66, "Scanning the data stream at a protocol level to detect a malware");**

blocking the identified packets from being transmitted to the target system **(Column 5, lines 5-8 "All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria");** and

Shetty discloses blocking received packet from being transmitted to the target system. Shetty does not disclose blocking one or more subsequently received packets from being transmitted to the target system when a severity of the attack exceeds a predetermined threshold, and the subsequently blocked packets including one or more of packets originating from the source system or directed to the target system.

However, Alampalayam, in the same field of endeavor of network security, discloses a system that blocks one or more subsequently received packets from being transmitted to the target system when a severity of the attack exceeds a predetermined threshold, and the subsequently blocked packets including one or more of packets originating from the source system or directed to the target system **(Page 1519, 2nd Column, "Step 3: Protection Framework" section, "For instance, once a DoS attack is detected, security level is increased. This causes the malicious nodes**

causing DoS attack to be disconnected or specific mobile IP address is blocked/automatically denied future connections from accessing the network.").

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to incorporate into the firewall of Shetty, the method of blocking subsequent packets from source system, as suggested by Alampalayam so that firewall of Shetty would not have to scan all incoming packets at a protocol level, instead it can simply look at the header of the packet and block it if it came from the attacking source, thus reducing the processing for firewall system of Shetty.

Regarding **Claims 2 and 12**, the rejection of claims 1 and 10 is incorporated and Shetty further discloses that monitoring the data packets includes determining at least one of identifying information or a type of communication associated with the monitored packets **(Column 3 lines 13-17, "As shown in FIG. 1, incoming network traffic 102 and outgoing network traffic 104 are filtered by one or more protocol filters, such as filters 106A-C. The protocol filters scan the traffic data stream for malwares")**.

Regarding **Clam 3**, the rejection of claim 2 is incorporated and further Shetty discloses wherein the identifying information includes at least one of a source Internet Protocol Address, a source port number, a destination Internet Protocol address, or a destination port number **(Column 3, lines 56-57,61 and Column 4 line 1, "Preferably, protocol scanner 108 will be capable of performing a number of function:" ... "Blocking an IP address or set of IP address" ... "Blocking ports")** *[Shetty's*

system is capable of blocking incoming packets based on the source IP address or just block traffic on certain ports]

Regarding **Claim 4**, the rejection of claim 2 is incorporated and further Shetty discloses that the type of communication includes at least one of File Transfer Protocol, Simple Mail Transfer Protocol, Telnet, Domain Name System, Windows Internet Name System, HyperText Transfer Protocol, Traceroute, instant messaging, or chat **(Column 3, lines 21-28, "Filter functionality is required for each protocol that is to be supported. For example, Post Office Protocol 3 (POP3) filter 106A scans the POP3 data stream, HyperText Transfer Protocol (HTTP) filter 106B scans the HTTP data stream, and File Transfer Protocol (FTP) filter 106C scans the FTP data stream. POP3 is a protocol used to retrieve e-mail from a mail server, HTTP is the underlying protocol used by the World Wide Web, and FTP is a protocol used on the Internet for sending files")**

Regarding **Claim 5**, the rejection of claim 1 is incorporated and Shetty further discloses that monitoring the packets includes using Transmission Control Protocol/Internet Protocol at an application layer **(Column 3, lines 58-60, "Scanning for computer malwares, such as viruses, Trojans and worms in the entire network TCP/IP protocol like HTTP, FTP, SMTP/POP3, etc.")**

Regarding **Claims 6, 13 and 19**, the rejection of claims 1, 10 and 16 is incorporated and Shetty further discloses that the severity of the attack is determined based on at least one of a frequency of the attack, a type of communication, a change in an amount of bandwidth, and a volume of received data packets **(Column 3, lines 65-67, "Blocking emails (stop network spamming): by scanning POP3 and SMTP protocols, protocol scanner 108 will be able to block emails from specified addresses.")** *[This is a detection of the severity of the attack is based on a type of communication i.e. blocking emails from specified addresses]*

Regarding **Claims 7, 14, and 20**, the rejection of claims 1, 10 and 16 is incorporated and Shetty further discloses wherein blocking the data packets from being transmitted to the target system includes instructing at least one of a router, a hub, a server, or a firewall to disable a communication channel. **(Column 5, lines 5-8 "All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria")**

Regarding **Claim 17**, the rejection of claim 16 is incorporated and Shetty further discloses that the that the received packets are monitored transparently in real-time **(Column 1, lines 58-60, "Malware scanning of data that is being transferred or downloaded to a computer system")** [It can be seen that security configuration of

Shetty's system that includes router/firewall and gateway system that is responsible for scanning incoming data is transparent to both the data receiving and sending host]

Regarding **Claim 18**, the rejection of claim 16 is incorporated and further Shetty discloses that the received packets are monitored after being stored in a storage buffer **(Column 7, lines 22-27, "Memory 408 includes protocol scanner 410, which includes at least one protocol filter, such as protocol filters 412A and 412B, application programs 414, and operating system 412. Protocol scanner 410 scans for network traffic for malwares and then forwards the scanned data to workstation computers and/or workstation computer applications")**

Regarding **Claim 23**, Shetty discloses a computer system configured for detecting and preventing attacks directed at target device **(Column 1, lines 6-8, "The present invention relates to a method, system and computer program product for detecting computer malwares that scans network traffic at the protocol level"),** comprising:

at least one terminal device **(Figure 3, Numeral 312A, "WORKSTATION");**

at least one server **(Figure 3, Numeral 310, "PROTOCOL SCANNER")** coupled to a computer network **(Fig. 3, Numeral 302, "Network")** and to the terminal device **(Fig. 3, Numeral 312A, "Workstation")**, the server operable to monitor packets directed to the terminal device, the server having one or more modules **(It is implied**

that firewall contains software modules that does the scanning of incoming packets) including:

a detection module that receives attack signatures associated with attacks directed at the terminal device packets and monitors received packet to identify one or more of the packets that include information associated with the attack signatures **(Column 1, lines 58-60, "Malware scanning of data that is being transferred or downloaded to a computer system")** ;

a scanning module that evaluates the packets to determine a severity of an attack on the terminal device **(Column 1, lines 65-66, "Scanning the data stream at a protocol level to detect a malware")**;

a blocking module that identifies a source of the identified packets, instructs at lease one switching device to block the identified packets from being transmitted to the terminal device **(Column 5, lines 5-8 "All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria")**.

Shetty discloses blocking received packet from being transmitted to the target system using a firewall. Shetty does not disclose blocking one or more subsequently received packets from being transmitted to the target system when a severity of the attack exceeds a predetermined threshold, and the subsequently blocked packets including one or more of packets originating from the source system or directed to the terminal device.

However, Alampalayam, in the same field of endeavor of network security, discloses a system that blocks one or more subsequently received packets from being transmitted to the target system when a severity of the attack exceeds a predetermined threshold, and the subsequently blocked packets including one or more of packets originating from the source system or directed to the target system **(Page 1519, 2nd Column, "Step 3: Protection Framework" section, "For instance, once a DoS attack is detected, security level is increased. This causes the malicious nodes causing DoS attack to be disconnected or specific mobile IP address is blocked/automatically denied future connections from accessing the network.")**.

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to incorporate into the firewall of Shetty, the method of blocking subsequent packets from source system, as suggested by Alampalayam so that firewall of Shetty would not have to scan all incoming packets at a protocol level, instead it can simply look at the header of the packet and block it if it came from the attacking source, thus reducing the processing for firewall system of Shetty.

Regarding **Claim 25**, the rejection of claim 23 is incorporated and further Shetty discloses a database coupled to the server **(Column 3, lines 61-67 and Column 4, lines 1-13)** *[Since the protocol scanner is capable of blocking data based on IP address or specific e-mail address, specific block and specific URLs, then it must have a database with all the entries of the IP addresses, e-mail address, port numbers and URLs to block]*

Regarding **Claim 26**, the rejection of claim 23 is incorporated and further Shetty discloses that the detection module monitors the received packets by determining at least one of identifying information or a type of communication associated with the monitored packets. **(Column 3 lines 13-17, "As shown in FIG. 1, incoming network traffic 102 and outgoing network traffic 104 are filtered by one or more protocol filters, such as filters 106A-C. The protocol filters scan the traffic data stream for malwares").**

Regarding **Claim 27**, the rejection of claim 23 is incorporated and further Shetty discloses that the scanning module determines the severity of the attack based on at least one of a frequency of the attack, a type of communication, a change in an amount of bandwidth, or a volume of the received data packets **(Column 3, lines 65-67, "Blocking emails (stop network spamming): by scanning POP3 and SMTP protocols, protocol scanner 108 will be able to block emails from specified addresses.")** *[This is a detection of the severity of the attack based on a type of communication i.e. blocking emails from specified addresses].*

Regarding **Claim 28**, the rejection of claim 23 is incorporated and Shetty further discloses that the blocking module blocks data packets from being transmitted to the terminal device by instructing at least one of a router, a hub, a server, or a firewall to disable a communication channel **(Column 5, lines 5-8 "All messages entering or**

leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria").

Regarding **Claims 8, 21 and 30**, the rejection of claims 1, 16 and 23 is incorporated and the combination of Shetty and Alampalayam as applied to the rejection of Claim 1, 16 and 23 does not explicitly teaches the step of notifying the source system the attack has been detected and that packets subsequently sent from the source system will be blocked.

However, Alampalayam in the same reference further discloses the step of notifying the source system the attack has been detected and that packets subsequently sent from the source system will be blocked **(Page 1519, "Step 3: Protection Framework" section, "If one require a message to be sent back to node (agent), the redirection feature would be used instead of deny feature, to redirect specific document to specific node (agent)").**

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to notify a user or administrator of the virus source computer as suggested by Alampalayam, after detecting and blocking the virus in Shetty's system *so that the administrative or user of the source computer from where the virus was generated can take corrective action to clean his/her system or to let him/her know why the connection is refused or blocked by router/firewall of the target system.*

Regarding **Claim 31**, the rejection of claim 3 is incorporated and the combination of Shetty and Alampalayam further discloses that the subsequently blocked packets including packets associated with one or more of the source Internet Protocol address, the source port number, the destination Internet Protocol address, or the destination port number **(Page 1519, 2nd Column, "Step 3: Protection Framework" section, "For instance, once a DoS attack is detected, security level is increased. This causes the malicious nodes causing DoS attack to be disconnected or specific mobile IP address is blocked/automatically denied future connections from accessing the network.")**.

Claims 9, 11, 15, 22, 24 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shetty in view of Alampalayam and further in view of Lachman, III et al. (US 2002/0166063).

Regarding **Claims 9, 15, 22 and 29**, rejections of claims 1, 14, 16, and 23 are incorporated and the combination of Shetty and Alampalayam teaches blocking data packets. The combination does not teach that the subsequently received packet are blocked from being transmitted to the target system for a predetermine amount of time.

However, Lachman, III et al., in the same field of endeavor of network security, discloses the data packets are blocked from entering the target system for a predetermined amount of time (Paragraph 0125, "If the flooding is of the single-source type, no packets will be routed from that source to the victim IP address for the specified block time).

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to block the data packets as disclosed by Shetty for only a predetermined amount of time as taught by Lachman, III et al. to *"prevent network flood interruptions without disrupting normal network operations" (Paragraph 0002, Lachman, III et al.)*

Regarding **Claims 11 and 24**, rejections of claims 10 and 23 are incorporated and the combination of Shetty and Alampalayam doesn't disclose a log of the packets identified as including the information associated with the attack signatures.

However, Lachman, III et al. further discloses a log-creating module that is adapted to create a log of the received data packets having the attack signatures **(Paragraph 0105, "if the network load reaches the set threshold, then system 106 can launch a countermeasure routine and can log the time of the flood, the time of the countermeasure deployment, and the source and destination of the offending packet (s).")**

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to create a log, as taught by Lachman, III et al., of the received data packets having the attack signature in the system of Shetty so that *the source of the offending packet **(Lachman, III et al., Paragraph 0105)** can be added to the blocking list of Shetty's router/firewall so that "the source will not [be] able to send or receive any data from the protected corporation network" **(Shetty, Column 3, lines 62-64).***

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yogesh Paliwal whose telephone number is (571) 270-1807. The examiner can normally be reached on M-F: 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

YP
7/29/2007

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100